ANALISIS UJI KUALITAS KEAMANAN WEBSITE PPDB SMK X MENGGUNAKAN METODE ISAAF

[1]Desi Susanti, [2]Sriyanto*

[1]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, desi5267@guru.smk.belajar.id
[2]Fakultas Ilmu Komputer, Institut Informatika dan Bisnis Darmajaya, sriyanto@darmajaya.ac.id

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah mendorong lembaga pendidikan, termasuk Sekolah Menengah Kejuruan (SMK) untuk menghadirkan sistem Penerimaan Peserta Didik Baru (PPDB) melalui platform daring.Kehadiran website Penerimaan Peserta Didik Baru (PPDB) sebagai media utama interaksi menuntut Keamanan siber yang handal mencakup perlindungan terhadap data sensitif peserta didik, integritas informasi dan ketersediaan layanan.
Penelitian ini juga bertujuan untuk melakukan uji kualitas keamanan pada website PPDB SMK X melalui pendekatan *Information System Security Assessment Framework (ISAAF)*. Pemindaian dilakukan untuk mengidentifikasi potensi risiko keamanan yang mungkin terdapat pada situs web ini. Dalam rangka mendukung tujuan tersebut dilakukan pemeriksaan *header HTTP*, identifikasi kerentanan *server-side software*, dan evaluasi terhadap kebijakan keamanan yang diimplementasikan pada situs web PPDB SMK X.
Hasil pemindaian menunjukkan bahwa website PPDB SMK X dapat diakses dengan baik tanpa masalah besar. Meskipun ditemukan beberapa rekomendasi terkait pengaturan header keamanan dan beberapa kerentanan pada *server-side software* namun secara keseluruhan tidak ada masalah signifikan yang dapat membahayakan keamanan situs web ini. Dengan memperkuat keamanan siber pada website PPDB SMK X peneliti berharap dapat memberikan kontribusi dalam pengembangan kebijakan keamanan informasi di lembaga pendidikan berbasis teknologi informasi sekaligus memberikan panduan untuk perbaikan dan peningkatan keamanan siber di masa mendatang.

Kata Kunci: Keamanan Siber, Web , PPDB, Sekolah Menengah Kejuruan (SMK), ISAAF

ABSTRACT

The development of information and communication technology has prompted educational institutions, including Vocational High Schools (SMK), to implement the New Student Admission System (PPDB) through an online platform. The presence of the New Student Admission System (PPDB) website as the main interaction medium demands a robust cyber security, encompassing the protection of sensitive student data, information integrity, and service availability.
This research aims to conduct a security quality assessment on the PPDB SMK X website using the Information System Security Assessment Framework (ISAAF) approach. Scanning is performed to identify potential security risks that may exist on this website. In supporting this objective, examinations of HTTP headers, identification of server-side software vulnerabilities, and evaluation of the security policies implemented on the PPDB SMK X website are conducted.
The scanning results indicate that the PPDB SMK X website can be accessed smoothly without significant issues. Although some recommendations are made regarding security header settings and a few vulnerabilities in server-side software, overall, there are no significant problems that could jeopardize the security of this website. By strengthening cyber security on the PPDB SMK X website, researchers hope to contribute to the development of information

Keywords: *Cyber Security, Website, PPDB, Vocational High School (SMK), ISAAF*

PENDAHULUAN

Di era digital yang semakin maju, keberadaan website sebagai salah satu sarana informasi dan interaksi menjadi sangat penting, terutama dalam konteks Penerimaan Peserta Didik Baru (PPDB) Sekolah Menengah Kejuruan (SMK) X. Sebagai lembaga pendidikan yang berbasis teknologi informasi dan mengedepankan sistem pembelajaran berbasis *ICT*, sekolah memiliki tanggung jawab besar untuk menyelenggarakan sistem penerimaan peserta didik baru dengan efisien dan menjaga keamanannya melalui website resminya. Website atau situs juga dapat diartikan sebagai kumpulan halaman yang menampilkan informasi data teks, data gambar, data animasi, suara, video, dan gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman atau hyperlink[1].

Kerentanan dalam membangun sistem jaringan komputer bisa berupa konfigurasi yang salah, prosedur yang kurang memadai, personel yang tidak berpengalaman atau tidak terlatih [2]. Sistem keamanan komputer pun menjadi penting karena berkaitan dengan data pribadi (*Privacy*), integritas (*Integrity*), hak akses atau verifikasi (*Autentication*), kerahasiaan (*Cofidentiality*) dan ketersediaan (*Availability*)[3] .Maka dalam menghadapi ancaman keamanan di dunia digital, penting untuk melakukan uji kualitas keamanan terhadap website penerimaan peserta didik baru di sekolah X. Penelitian ini bertujuan untuk melakukan uji kualitas keamanan pada website PPDB SMK X melalui pendekatan *Information System Security Assessment Framework (ISAAF*). Metode ISSAF dipilih karena sesuai dengan tujuan penelitian dan bersifat open source, sehingga bebas digunakan oleh siapa saja. Selain itu ISSAF memiliki kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain[4].

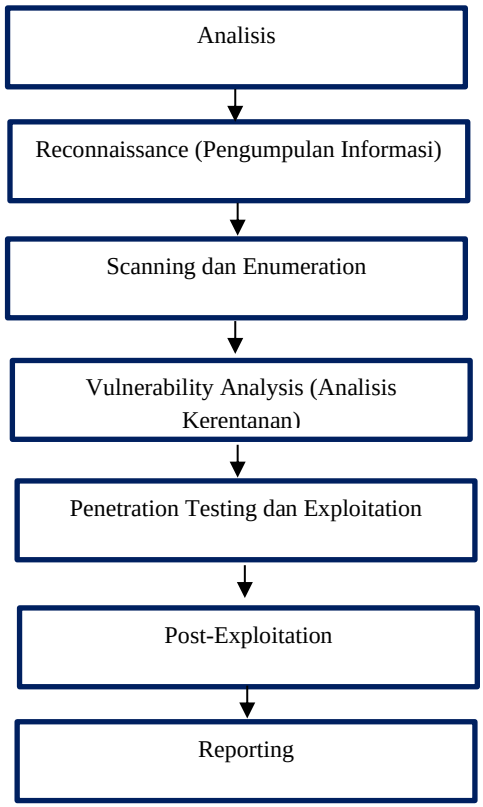
Dengan demikian, penelitian ini mencoba mengisi kesenjangan pengetahuan dengan memberikan kontribusi dalam memahami dan meningkatkan keamanan siber pada website penerimaan peserta didik baru di Sekolah Menengah Kejuruan X melalui serangkaian pengujian *penetration test*. Termasuk analisis *header HTTP*, pemeriksaan kerentanan *server-side software* dan evaluasi kebijakan keamanan yang diimplementasikan.

Penelitian mengenai *penetration testing* menggunakan *framework* ISAAF pernah dilakukan sebelumnya oleh I Gede Ary Suta Sanjaya, yang menjelaskan mengenai pengujian keamanan website lembaga X melalui *penetration testing framework* ISSAF meliputi sembilan asesmen pengujian yaitu *Information Gathering, Network Mapping, Vulnerability Identification, Penetration, Gaining Access and Privilege Escalation, Enumerating Further, Compromise Remote User/Sites, Maintaining Access, dan Covering Tracks*[5]. Framework ISSAF cukup banyak digunakan untuk pengujian keamanan sistem melalui metode *penetration testing*. Sulis Andriyani pada penelitiannya melakukan Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode *Penetration Testing* Dan *Framework* Issaf Pada Website SMK Al-Kautsar. Salah satu pengujiannya yaitu dengan menggunakan metode *penetration testing*. *Penetration testing* merupakan sebuah simulasi serangan yang terkendali dengan tujuan untuk melakukan identifikasi kerentanan terhadap aplikasi, jaringan, dan cabang system informasi[6].

Maka pemahaman yang mendalam terhadap keamanan website PPDB SMK X melalui pendekatan ISAAF diharapkan dapat memberikan pembaruan kebijakan dan tindakan preventif yang relevan guna menghadapi tantangan keamanan di dunia digital. Dengan demikian, penelitian ini tidak hanya memberikan manfaat akademis, tetapi juga dapat menjadi dasar untuk pengembangan kebijakan keamanan informasi yang lebih baik di lingkungan pendidikan berbasis teknologi informasi.

METODOLOGI PENELITIAN

Framework Information Systems Security Assessment Framework (ISSAF) adalah sebuah kerangka kerja keamanan sistem informasi yang dirancang untuk memberikan struktur yang terstruktur untuk mengevaluasi dan meningkatkan keamanan sistem informasi[7]. Berikut adalah tahapan penggambaran penelitian penetration testing menggunakan *Framework* ISSAF:



Gambar 1. Metodologi Penelitian

2.1 Analisis

Tahap analisis bertujuan untuk mengidentifikasi celah kerawanan[8].

2.2 *Reconnaissance* (Pengumpulan Informasi)

Fase ini juga dikenal sebagai *foot-printing.* Ini adalah langkah pengumpulan informasi secara pasif dan persiapan untuk melakukan uji penetrasi yang sebenarnya. Dimulai dengan mengumpulkan sebanyak mungkin informasi tentang organisasi (sistem dan jaringan) yang sedang diuji[9].

2.3 *Scanning* dan *Enumeration*

Port scanning bertujuan untuk menemukan celah keamanan yang berada pada *server* dengan mencari *port* yang berstatus terbuka pada *server*. Celah keamanan yang dicari pada tahap *port scanning* ada 4 jenis yaitu *port, status, service* yang berjalan dan versi dari sistem operasi yang digunakan. Celah keamanan yang ditemukan digunakan untuk melakukan peretasan pada sistem *server*. Celah keamanan juga digunakan untuk melakukan *planning* untuk menentukan jenis serangan dan *tools* yang akan digunakan untuk melakukan serangan pada sistem *server*[10].

2.4 *Vulnerability Analysis* (Analisis Kerentanan)

Tahap *vulnerability analysis* merupakan tahapan pemindaian website target untuk mengetahui kerentanan keamanan didalamnya [5].

2.5 *Penetration Testing* dan *Exploitation*

Penetrasi adalah pengujian keamanan untuk menentukan kerentanan yang terdapat pada sistem. Kerentanan yaitu suatu kelemahan yang dapat diserang sehingga mengganggu atau

mendapatkan akses ke sistem dan data informasi didalamnya[11]. Pada proses *penetration testing* dilakukan berdasarkan kerentanan yang ditemukan pada tahap *vulnerability analysis*[12]. Sedangkan *Exploitation* merupakan kerentanan yang sudah ada dijadikan bahan untuk masuk dan melakukan eksploitasi lebih lanjut. Tahap ini akan mencoba semaksimal mungkin apa saja yang bisa dilakukan dan didapatkan dari sistem secara ilegal[13].

2.6 *Post-Exploitation*

Setelah fase eksploitasi selesai, penting untuk mendokumentasikan proses dan metodologi yang digunakan dalam fase eksploitasi serta daftar semua sumber daya yang dikompromi (misalnya, akun, sistem, aplikasi, dll.) [9]. Fase *Post Exploitation* juga bertujuan untuk menentukan nilai dari sistem yang terekspos dan untuk menjaga kontrol sistem agar dapat terus berjalan. Nilai dari sistem akan ditentukan dari sensitivitas data yang disimpan di dalamnya dan peranan sistem tersebut di dalam jaringan yang diekspos[14].

2.7 *Reporting*

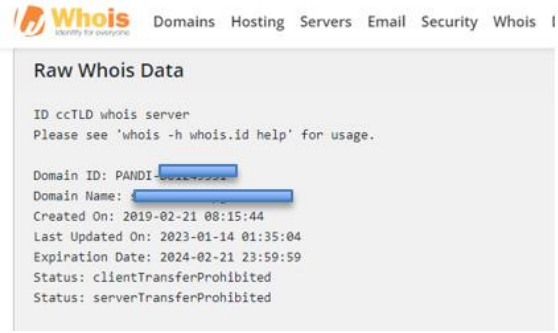
Mengidentifikasi dan mendokumentasikan hasil. Hal terpenting dalam tahap ini adalah memberikan gambaran umum hingga rinci status sistem berdasarkan jenis dan tingkat kerentangan sistem terhadap serangan. Dari hasil ini pemangku kepentingan juga diberi gambaran bagaimana memprioritaskan dan menerapkan tindakan korektif untuk kerentanan yang diketahui yang dilaporkan[13].

HASIL DAN PEMBAHASAN

Dalam penelitian ini, pembahasan mengenai hasil pengujian *Penetration Testing* menggunakan *Framework* ISSAF mencakup evaluasi hasil pengujian serta pemaparan rekomendasi berdasarkan temuan tersebut.

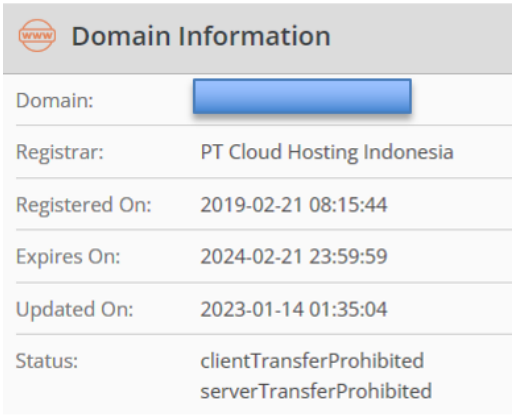
3.1 Analisis

Pada fase ini penulis menganalisis dan mendapatkan informasi dari target berupa *ip address public* dan *port* yang digunakan. Dalam hal ini penulis menggunakan website http://whois.net. Hasil *scanning* dengan Whois dapat di lihat pada gambar di bawah ini:



Gambar 2. Hasil pemindaian Whois Domain1

Dari gambar 3.1 Whois Domain memberikan informasi mengenai gambaran status, masa berlaku, dan pembatasan transfer untuk domain tersebut. Informasi output dari layanan whois untuk domain "X" pada *server whois ccTLD (Country Code Top-Level Domain)* Indonesia adalah Domain ID: PANDI-XXX Ini adalah identifikasi unik untuk domain di *registry ccTLD* Indonesia (PANDI), nama domainnya yaitu X kemudian statusnya *clientTransferProhibited* menunjukkan bahwa transfer domain oleh klien tidak diizinkan.

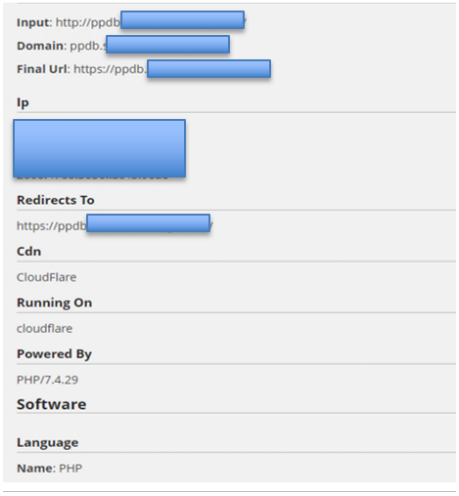


Gambar 3. Hasil pemindaian Whois Domain2

Dari gambar 3.2 dapat diperhatikan bahwa hasil pemindaian menggunakan alat Whois Domain memberikan informasi Domain "X" didaftarkan pada 21 Februari 2019, melalui *registrar* PT Cloud Hosting Indonesia. Saat ini, status domain ini adalah "*clientTransferProhibited*" dan "*serverTransferProhibited*," yang berarti ada pembatasan untuk transfer domain baik dari sisi klien maupun *server*. Informasi perpanjangan domain menunjukkan bahwa domain ini akan berakhir pada 21 Februari 2024. Terakhir kali diperbarui pada 14 Januari 2023.

3.2 *Reconnaissance* (Pengumpulan Informasi)

Pada tahap *Reconnaissance* (Pengumpulan Informasi), pengujian dilakukan dengan mengumpulkan informasi umum mengenai website target.Ini dilakukan dengan memasukkan domain website target ke tool SiteGuarding guna mendapatkan data yang relevan.



Gambar 4. Hasil pemindaian menggunakan SiteGuarding

Hasil dari pengujian ini Awalnya, situs diakses melalui URL http://ppdbX. Namun terjadi pengalihan (redirect) ke URL akhir yang lebih aman menggunakan protokol HTTPS: https://ppdbX Pada alamat IP terdapat empat alamat IP yang terkait dengan domain tersebut, termasuk alamat IPv4 dan IPv6. TCP/IP memiliki kelas-kelas IP *Address* (alamat IP) yang terdiri dari kelas A, B, C, D, dan E. Setiap kelas memiliki ukuran dan jumlah yang berbeda[15] .Kemudian situs menggunakan layanan CDN dari *CloudFlare*. Layanan ini membantu dalam mendistribusikan konten secara efisien dan meningkatkan keamanan.
Situs dijalankan di atas *platform Cloudflare*, menggunakan PHP sebagai teknologi *server-side scripting* dengan versi 7.4.29.

Dalam pengujian ini *Cloudflare* sebagai CDN membuktikan bahwa web PPDB SMK X memanfaatkan layanan untuk keamanan dan kinerja yang lebih baik. Selain itu, penggunaan HTTPS (*secure*) melalui protokol versi terbaru menunjukkan kepedulian terhadap keamanan komunikasi dengan pengguna. *Software server* yang digunakan adalah PHP versi 7.4.29, yang umumnya digunakan untuk pengembangan web dinamis.

3.3 Scanning dan Enumeration

Pada tahap ini di lakukan proses pengidentifikasian dan pemetaan sistem, jaringan, atau layanan yang beroperasi di dalamnya. Tujuannya adalah untuk mendapatkan informasi tentang target yang dapat digunakan untuk melaksanakan serangan atau penilaian keamanan. Tools yang digunakan yaitu Nmap (*Network Mapper*) untuk melakukan proses pemeriksaan jaringan pengidentifikasian host, layanan, dan port-port yang aktif dalam suatu sistem.

Ini juga akan digunakan untuk menemukan dan menyalahgunakan kerentanan dalam suatu sistem.Adapun hasil pemindaian IP menggunakan NMap sebagai berikut:

```
Starting Nmap 7.40 ( https://nmap.org ) at 2024-01-01 07:31 UTC
Nmap scan report for [redacted]
Host is up (0.0019s latency).
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
```

Gambar 5. Hasil pemindaian menggunakan NMap1

Hasil pemindaian Nmap memberikan informasi tentang status port pada host dengan alamat IP pada waktu tertentu.

Host dengan IP X dinyatakan "*up*," yang berarti host tersebut responsif terhadap permintaan Nmap.Port 21 (FTP) dinyatakan sebagai "*filtered*," yang berarti Nmap tidak dapat menentukan apakah port tersebut terbuka atau tertutup karena beberapa alasan, seperti *firewall* atau konfigurasi jaringan.

Port 22 (SSH) juga dinyatakan "*filtered*."
Port 23 (Telnet) juga dinyatakan "*filtered*."
Port 80 (HTTP) dinyatakan *"open*," yang berarti port tersebut aktif dan menerima koneksi.
Port 110 (POP3) dinyatakan "*filtered."*
Port 143 (IMAP) dinyatakan "*filtered."*
Port 443 (HTTPS) dinyatakan "*open."*
Port 3389 (MS-WBT-Server) dinyatakan "*filtered."*
untuk *Latency host* tercatat sekitar 0.0019 detik.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2024-01-01 08:20 UTC
Nmap scan report for [redacted]
Host is up (0.0019s latency).
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
80/tcp   open     http
110/tcp  filtered pop3
143/tcp  filtered imap
443/tcp  open     https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
```

Gambar 6. Hasil pemindaian menggunakan NMap2

Sedangkan hasil pemindaian Nmap dengan alamat IP X yaitu Host dengan IP X dinyatakan "*up,*" yang berarti host tersebut responsif terhadap permintaan Nmap.

Port 21 (FTP) dinyatakan sebagai "*filtered*," yang berarti Nmap tidak dapat menentukan apakah port tersebut terbuka atau tertutup karena beberapa alasan, seperti firewall atau konfigurasi jaringan.
Port 22 (SSH) juga dinyatakan "*filtered*."
Port 23 (Telnet) juga dinyatakan "*filtered."*
Port 80 (HTTP) dinyatakan "*open*," yang berarti port tersebut aktif dan menerima koneksi.
Port 110 (POP3) dinyatakan "*filtered."*
Port 143 (IMAP) dinyatakan "*filtered."*
Port 443 (HTTPS) dinyatakan "*open."*
Port 3389 (MS-WBT-*Server*) dinyatakan "*filtered."*
Latency host tercatat sekitar 0.0017 detik.

3.4 *Vulnerability Analysis* (Analisis Kerentanan)

Pengujian pada tahap *vulnerability identification* dilakukan dengan memindai kerentanan keamanan yang terdapat pada website target. Pemindaian kerentanan dilakukan dengan menggunakan *tool Vega Vulnerability Scanner* yang diuji pada domain utama dan subdomain website target.

Gambar 7. Risk Rating

Hasil pemindaian menunjukkan bahwa situs web memiliki tingkat risiko yang tinggi. Dari temuan yang diidentifikasi, risiko tersebut dapat diperinci sebagai berikut:

a. Kerentanan Perangkat Lunak *Server*

Level Risiko: Tinggi
Terdapat beberapa kerentanan pada perangkat lunak *server*, termasuk kerentanan dengan tingkat keparahan yang tinggi. Diperlukan pembaruan perangkat lunak untuk mengatasi risiko ini.

b. *Header* Keamanan yang Hilang

Level Risiko: Rendah
Beberapa header keamanan yang kritis hilang, termasuk *Content Security Policy*, *Strict-Transport-Security*, *X-Frame-Options*, dan *X-Content-Type-Options*. Meskipun risiko ini dinilai rendah, tetapi penting untuk menambahkan header keamanan ini untuk melindungi situs dari serangan potensial.

c.*Vulnerabilitas* Kebijakan Akses Klien
Level Risiko: Rendah
Tidak ditemukan masalah dengan kebijakan akses klien, yang dapat mencakup pembatasan akses berdasarkan perangkat atau lokasi. Risiko ini dinilai rendah.
d.Ketidakadaan File robots.txt
Level Risiko: Rendah
Meskipun tidak ada file robots.txt yang ditemukan, ini bukan masalah kritis. Risiko ini dinilai rendah.
e. Ketidakadaan File security.txt
Level Risiko: Rendah
Tidak ditemukan file security.txt, yang dapat berisi informasi kontak untuk melaporkan kerentanan keamanan. Risiko ini dinilai rendah.
f. Penggunaan Sertifikat yang Tidak Dipercayai
Level Risiko: Rendah
Tidak ditemukan penggunaan sertifikat yang tidak dipercayai. Ini adalah temuan positif dan risiko ini dinilai rendah.
g. Metode *Debug* HTTP yang Diaktifkan
Level Risiko: Informasi
Tidak ditemukan metode debug HTTP yang diaktifkan. Ini adalah temuan positif dan tidak menimbulkan risiko signifikan
h. Komunikasi yang Aman
Level Risiko: Informasi
Meskipun disebut "Tidak Ada yang Ditemukan," hasil ini tidak memberikan informasi spesifik tentang keamanan komunikasi. Ini memerlukan peninjauan lebih lanjut.
i. Daftar Direktori
Level Risiko: Informasi
Tidak ditemukan daftar direktori, menunjukkan bahwa *server* tidak mengizinkan akses langsung ke struktur direktori.
j. Domain Terlalu Longgar untuk *Cookie*
Level Risiko: Informasi
Tidak ditemukan konfigurasi domain yang terlalu longgar untuk *cookie*. Ini adalah temuan positif dan tidak menimbulkan risiko signifikan.
k. *Flag HttpOnly pada Cookie*
Level Risiko: Informasi
Tidak ditemukan konfigurasi *flag HttpOnly* pada *cookie.* Ini adalah temuan positif dan tidak menimbulkan risiko signifikan.
l.*Flag Secure pada Cookie*
Level Risiko: Informasi
tidak ditemukan konfigurasi *flag Secure* pada *cookie*. Ini adalah temuan positif dan tidak menimbulkan risiko signifikan.
m. *Header HTTP Content Security Policy* yang Tidak Aman
Level Risiko: Informasi
Tidak ditemukan *header HTTP Content Security Policy* yang tidak aman. Ini adalah temuan positif dan tidak menimbulkan risiko signifikan.

Tabel 1. *Vulnerabilities Found For Server-Side Software*

Risk level	CVSS	CVE	Summary	Exploit	Affected Software
High	9.8	CVE-2022-37454	*The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected*	N/A	php 7.4.29

			cryptographic properties. This occurs in the sponge function interface.		
High	7.1	CVE-2022-31630	*In PHP versions prior to 7.4.33, 8.0.25 and 8.2.12, when using imageloadfont() function in gd extension, it is possible to supply a specially crafted font file, such as if the loaded font is used with imagechar() function, the read outside allocated buffer will be used. This can lead to crashes or disclosure of confidential information.*	N/A	php 7.4.29
High	6.8	CVE-2022-31625	*In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service.*	N/A	php 7.4.29
High	6.5	CVE-2022-31629	*In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications.*	N/A	php 7.4.29
High	6	CVE-2022-31626	*In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is allowed to supply host to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code execution vulnerability.*	N/A	php 7.4.29

Kerentanan-kerentanan pada tabel ini menghadapkan aplikasi terkena risiko akses tidak sah terhadap data rahasia dan mungkin terhadap serangan layanan tidak tersedia (*denial of service*). Penyerang dapat mencari atau membuat eksploitasi yang sesuai untuk salah satu kerentanan ini dan menggunakannya untuk menyerang sistem. Untuk menghindari hal tersebut sebaiknya meningkatkan perangkat lunak ke versi terbaru guna menghilangkan risiko dari kerentanan ini.

Tabel 2. *Risk Classification Vulnerabilities*

CWE	CWE-1026
OWASP Top 10 - 2013	*A9 - Using Components with Known Vulnerabilities*
OWASP Top 10 - 2017	*A9 - Using Components with Known Vulnerabilities*

Tingkat risiko keseluruhan dikategorikan sebagai "Tinggi," menunjukkan bahwa ada satu temuan risiko tinggi dan beberapa temuan risiko rendah serta informasi.Temuan melibatkan kerentanan pada perangkat lunak *server-side PHP,* dengan beberapa CVE yang merinci masalah-masalah potensial termasuk eksekusi kode arbitrer, bocoran informasi, dan kerentanan RCE *(Remote Code Execution*).Klasifikasi risiko mencakup CWE-1026 (Ketidakpastian Keamanan) serta status "Belum Dikonfirmasi."Temuan ini juga terkait dengan OWASP Top 10, yaitu A9 - Menggunakan Komponen dengan Kerentanan yang Diketahui versi 2013 dan 2017. Secara keseluruhan, hasil pemindaian menunjukkan tingkat risiko tinggi dan sebaiknya dilakukan tindakan perbaikan dengan segera untuk mengurangi potensi kerentanan pada perangkat lunak *server-side PHP*.

3.5 Penetration Testing dan Exploitation

Pengujian penetrasi adalah bagian penting dari penilaian keamanan dunia maya, dengan fokus pada potensi kerentanan yang terkait sistem yang ada[16] .

3.5.1 Missing Security Header: Content-Security-Policy

Tabel 3. *Missing Security Header: Content-Security-Policy*

URL	Evidence
https://ppdbX	*Response headers do not include the HTTP Strict-Transport-Security header*

Header HTTP Strict-Transport-Security memberi petunjuk kepada peramban untuk hanya menginisiasi koneksi aman (HTTPS) ke *server* web dan menolak segala upaya koneksi HTTP yang tidak terenkripsi. Ketidakhadiran *header* ini memungkinkan seorang penyerang untuk memaksa pengguna korban menginisiasi koneksi HTTP tidak terenkripsi ke server, membuka kemungkinan untuk menyadap lalu lintas jaringan dan mengekstrak informasi sensitif, seperti *session cookies*.

Tabel 4. : Risk Classification Security Header

CWE	CWE- 693
OWASP Top 10 - 2013	*A5 - Security Misconfiguration*
OWASP Top 10 - 2017	*A6 - Security Misconfiguration*

Header HTTP Strict-Transport-Security memberi petunjuk kepada peramban untuk hanya menginisiasi koneksi aman (HTTPS) ke *server* web dan menolak segala upaya koneksi HTTP yang tidak terenkripsi. Ketidakhadiran header ini memungkinkan seorang penyerang untuk memaksa pengguna korban menginisiasi koneksi HTTP tidak terenkripsi ke *server*, membuka kemungkinan untuk menyadap lalu lintas jaringan dan mengekstrak informasi sensitif, seperti *session cookies.*

3.5.2 Missing security header: X-Frame-Options

Tabel 5 : *Missing security header: X-Frame-Options*

URL	Evidence
https://ppdbX	Response headers do not include the HTTP X-Frame-Options security header

Ketika hasil pemindaian menyebutkan *"Missing security header: X-Frame-Options*" untuk URL https://ppdbX itu berarti bahwa *server* web di alamat tersebut tidak menyertakan *header* keamanan *HTTP X-Frame-Options* dalam respons HTTP-nya .*Header* keamanan ini memberikan instruksi kepada peramban web tentang cara menangani situs web dalam elemen *iframe* di halaman

web lain. Tanpa *header* ini, situs web dapat disematkan dalam bingkai di situs web lain, yang dapat meningkatkan risiko serangan *Clickjacking*. *Clickjacking* adalah jenis serangan yang terjadi pada aplikasi berbasis website. Serangan ini akan membuat korbannya secara tidak sengaja mengklik sebuah elemen pada halaman web yang seharusnya tidak ingin diklik. Serangan ini biasanya dilakukan dengan memanipulasi tampilan halaman website[6].

3.5.3 Missing security header: Referrer-Policy

Tabel 6 : *Missing security header: Referrer-Policy*

URL	Evidence
https://ppdbX	*Response headers do not include the Referrer-Policy HTTP security header as well as the tag with name 'referrer' is not present in the response*

Situs web https://ppdbX tidak menyertakan header keamanan HTTP *Referrer-Policy*. Ini berarti *browser* dapat mengirimkan informasi *referrer* yang lengkap ke situs web yang dituju ketika pengguna mengklik tautan dari halaman tersebut.

3.5.4 Missing security header: X-Content-Type-Options

Tabel 7 : *Missing security header: X-Content-Type-Options*

URL	Evidence
https://ppdbX	*Response headers do not include the X-Content-Type-Options HTTP security header*

Header keamanan *HTTP X-Content-Type-Options* memberikan petunjuk kepada *browser*, terutama *browser Internet Explorer*, untuk tidak melakukan "*MIME-sniffing*" atau "*content type sniffing"*. *MIME-sniffing* adalah proses di mana browser mencoba menentukan jenis konten (*Content-Type*) suatu file berdasarkan isinya, daripada hanya mengandalkan *header Content-Type* yang diberikan oleh server.Jika header *X-Content-Type-Options* tidak disertakan, *maka Internet Explorer* dapat mencoba menafsirkan kembali konten suatu halaman web (*MIME-sniffing*). Hal ini dapat membuka celah keamanan dan meningkatkan risiko serangan, *seperti Cross-Site Scripting (XSS)* atau *phishing*.

3.5.5 Server Software And Technology Found

Software / Version	Category
PHP 7.4.29	Programming languages
Cloudflare	CDN
HTTP/3	Miscellaneous
Bootstrap	UI frameworks
Lightbox	JavaScript libraries

Gambar 8. Scanning Results

Dari gambar 8 diketahui Informasi tentang perangkat lunak dan teknologi *server* yang ditemukan dapat memberikan wawasan kepada penyerang untuk merencanakan serangan yang

spesifik terhadap jenis dan versi perangkat lunak yang digunakan. Dalam hal ini, hasil pemindaian telah mengidentifikasi beberapa informasi berikut:

a.PHP 7.4.29 (*Programming languages*)

Ini menunjukkan versi PHP yang digunakan oleh server. Penyerang mungkin mencoba mengeksploitasi kerentanan yang diketahui dalam versi PHP ini.

b. *Cloudflare CDN (Content Delivery Network)*

Informasi ini mengindikasikan penggunaan *Cloudflare* sebagai CDN. Meskipun CDN bertujuan untuk meningkatkan kinerja dan keamanan, penyerang mungkin mencoba mengeksploitasi konfigurasi CDN atau mencari kerentanan yang mungkin ada.

c. HTTP/3 (*Miscellaneous)*

Menunjukkan bahwa server mendukung protokol HTTP/3. Penyerang mungkin mencari cara untuk mengeksploitasi atau memanfaatkan fitur-fitur tertentu yang terkait dengan versi protokol ini.

d. *Bootstrap UI frameworks*

Bootstrap adalah kerangka kerja antarmuka pengguna (UI framework) yang umum digunakan. Penyerang mungkin mencoba mengeksploitasi kerentanan yang diketahui dalam versi *Bootstrap* yang digunakan.

e.*Lightbox JavaScript libraries*

Lightbox adalah pustaka *JavaScript* untuk menampilkan gambar dengan antarmuka yang interaktif. Penyerang mungkin mencari kerentanan dalam pustaka ini untuk melancarkan serangan terhadap aplikasi.

3.6. *Post-Exploitation*

Potensial *post-exploitation* yang mungkin terkait dengan temuan keamanan hasil uji kualitas keamanan website adalah :

1. Eksploitasi Kerentanan *Server-Side Software*
   Jika kelemahan yang ditemukan dalam *server-side software*, seperti PHP, tidak segera diperbaiki, seorang penyerang dapat mencoba mengeksploitasi kerentanan tersebut untuk mendapatkan akses yang tidak sah atau mengakibatkan *denial of service*.
2. *DoS Attack* melalui *wp-cron.php*
   Jika tidak ada tindakan yang diambil terhadap temuan wp-cron.php, seorang penyerang dapat mencoba melancarkan serangan *Denial of Service (DoS)* dengan memicu permintaan berulang ke file tersebut.
3. Pemanfaatan Informasi *Header Server*
   Informasi *header server* yang terbuka dapat memberikan penyerang wawasan tambahan tentang lingkungan teknologi yang digunakan. Meskipun ini bukan *post-exploitation* secara langsung, informasi ini bisa digunakan untuk merencanakan serangan lebih lanjut yang ditargetkan.
4. Potensi Eksploitasi Kerentanan PHP
   Jika ada kerentanan di PHP atau ekstensi PHP tertentu, seorang penyerang dapat mencoba mengeksploitasi kerentanan tersebut untuk mendapatkan kontrol lebih lanjut atas server.

SIMPULAN

Hasil pemindaian situs web menunjukkan bahwa situs tersebut dapat diakses dengan baik tanpa masalah besar. Selama pemindaian, tidak ada kebijakan akses klien khusus yang ditemukan, tidak ada *file robots.txt* yang memberikan instruksi khusus kepada mesin telusur, dan tidak ada file *security.txt* yang memberikan informasi keamanan dan kontak darurat.

Selain itu, situs web menggunakan sertifikat keamanan yang dapat dipercayai untuk melindungi koneksi dengan pengguna. Tidak ada metode debug HTTP yang diaktifkan, yang positif untuk keamanan, dan tidak ada temuan terkait konfigurasi *cookie* yang terlalu longgar.

Pentingnya, situs web juga tidak mengaktifkan metode *listing* direktori yang dapat memberikan informasi struktur *internal file* dan folder. Konfigurasi *cookie*, termasuk pengaturan *flag HttpOnly* dan *Secure*, tampaknya telah diatur dengan baik untuk melindungi mereka dari potensi risiko keamanan.

Secara keseluruhan, meskipun ada beberapa rekomendasi umum, pemindaian ini tidak mengidentifikasi masalah besar yang dapat membahayakan keamanan situs web. Ini adalah tanda baik untuk pemilik situs web dan pengguna.

DAFTAR PUSTAKA

[1] A. Alfisyakhrin, I. Nawangsih, and I. Romli, "Sistem Pembayaran SPP pada SMK Berbasis Web Menggunakan Metode Waterfall," *Media Online)*, vol. 4, no. 2, pp. 1100–1110, 2023, doi: 10.30865/klik.v4i2.1314.

[2] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[3] M. V. Aguayo Torrez, "No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title," vol. 2, no. 4, pp. 506–519, 2021.

[4] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan Penetration Test Dan Issaf," *Transmisi*, vol. 24, no. 3, pp. 83–91, 2022, doi: 10.14710/transmisi.24.3.83-91.

[5] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.

[6] S. Andriyani, M. F. Sidiq, and B. P. Zen, "Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar," *J. Inform. Inf. Technol.*, vol. 8798, pp. 1–13, 2023.

[7] Z. A. Khan, N. S. H, M. Irsyad, and T. Darmizal, "Penetration Testing Information System Security Assessment Framework (ISSAF)," vol. 4, no. 3, pp. 1593–1601, 2023, doi: 10.30865/klik.v4i3.1503.

[8] S. U. Sunaringtyas and D. S. Prayoga, "Implementasi Penetration Testing Execution Standard Untuk Uji Penetrasi Pada," *Edu Komputika J.*, vol. 8, no. 1, pp. 48–56, 2021.

[9] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *J. Web Eng.*, vol. 21, no. 7, pp. 2187–2208, 2022, doi: 10.13052/jwe1540-9589.2178.

[10] F. R. Mahtuf, P. Hatta, and E. S. Wihidiyat, "Pengembangan Laboratorium Virtual untuk Simulasi Uji Penetrasi Sistem Keamanan Jaringan," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 4, no. 1, p. 17, 2019, doi: 10.31328/jointecs.v4i1.1000.

[11] A. Bimandaru and A. Nugroho, "ANALISIS PENGUJIAN PENETRASI PADA LAYANAN HOSTING (Studi kasus : Blogspot , Wordpress dan Shared Hosting)," vol. 13, no. 1, 2023.

[12] M. R. Ramdani, N. Heryana, and Y. S. A. Irawan, "Penetration Testing pada Website Universitas Singaperbangsa Karawang Menggunakan Open Web Application Security Project (OWASP)," *J. Pendidik. dan Konseling*, vol. 4, no. 3, pp. 5522–5529, 2022, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/6353

[13] B. Setiawan, F. Samopa, I. A. Akbar, N. A. Sani, B. C. Hidayanto, and Y. S. Dharmawan, "Pendampingan Analisis Vulnerability dan Hardening pada Website Pemerintah Kota Surabaya," *Sewagati*, vol. 7, no. 6, pp. 897–906, 2023, doi: 10.12962/j26139960.v7i6.624.

[14] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: 10.32722/multinetics.v6i2.3432.

[15] A. M. Kurnia *et al.*, "Implementasi+Keamanan+Jaringan+Komputer+Menggunakan+Standard+Access+Control +List+pada+Jaringan+LAN+dan+WLAN," vol. 21, no. 1, pp. 38–53, 2023.

[16] F. Fachri, A. Fadlil, and I. Riadi, "Analisis Keamanan Webserver menggunakan Penetration Test," *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.